United Nations A/HRC/26/NGO/5

General Assembly

Distr.: General
2 June 2014

English only

Human Rights Council
Twenty-sixth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Reporters Without Borders International, a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[21 May 2014]

* This written statement is issued, unedited, in the language(s) received from the submitting non-governmental organization(s).

GE.14-03856 (E)
1403856

Please recycle

The era of digital mercenaries

The internet is an invaluable tool for human rights defenders, journalists, netizens and citizen journalists. They use the internet to research and circulate news, communicate with each other, store data and disseminate opinions. The global network has become indispensable to the exercise of freedom of information.

But the internet is has also become a powerful tool for governments to monitor, identify, localize and censor individuals, especially journalists and netizens, who circulate information they prefer not to make public. Monitoring of the internet and its users has become a daily, massive reality. Many governments systematically monitor all those who provide information, a practice that gives rise to serious violations of human rights and freedom of information.

Though internet censorship and surveillance limit the exercise of fundamental rights and freedoms, online freedom of expression enables free debate on matters of general interest, such as sustainable development, good government and protection of democratic rights. Expansion of surveillance has become a major concern in the protection of human rights, and freedom of expression and information in the 21st century.

THE SURVEILLANCE BUSINESS; DIGITAL MERCENARIES

Companies that develop and sell internet surveillance technology have a major stake in this entire issue. Online censorship and surveillance by governments would be impossible without tools developed by private firms. Many of these companies, acting from entirely commercial motives, agree to work with authoritarian governments and to sell them technologies that enable the monitoring of citizens, the opposition and journalists. These governments make massive use of these products to violate human rights and the freedom of information. The companies cannot pretend not to know how their technology is used.

Companies in this business are truly digital era mercenaries, sharing a market worth more than $5 billion in 2011, according to Wikileaks.

The firms offer their services to a number of governments. In 2013, Reporters Without Borders designated five companies *Gamma, Trovicor, Hacking Team, Amesys* and *Blue Coat* – as Internet Enemies.'' They have sold surveillance tools to authoritarian regimes including Bahrain, Syria, Vietnam and Iran. In Ethiopia, the Information Network Security Agency has tracked journalists as far away as the United States with the help of software from *Hacking Team,* an Italian company. ZTE, a Chinese firm, has become the leading supplier of modems and routers to Uzbekistan.

Beyond the work of companies specializing in surveillance technology, the major internet players are also guilty of complicity in human rights violations committed on a massive scale. In 2005, information provided by *Yahoo!* to the Chinese government prompted the arest of journalist Shi Tao, who was sentenced to 10 years in prison for having disclosed ''state secrets.'' *Yahoo!* Voluntarily turned over a major quantity of data that allowed identification of the journalist as well as the nature and content of his electronic communications. Likewise, the *Sina/Weibo* Chinese microblogging company collaborates with the Chinese government in intercepting and censoring messages, thereby becoming an accomplice to the subsequent persecution of the authors.

Ambivalent behaviour of Western democracies

Most of the companies that develop and sell surveillance technology are based in democratic countries. There, laws exist to protect human rights, and freedom of information and expression, as well as privacy. The five companies that Reporters Without Borders designated in 2013 as ''Internet Enemies'' are based in the United Kingdom, Germany, Italy, France and the United States. These countries close their eyes to the nature of these businesses, and sometimes even grant trade preferences for exports to authoritarian countries.

Another illustration of the ambivalent behaviour of Western democracies: the ISS World, Technology Against Crime and Milipol trade fairs, which amount to trafficking in surveillance technology. These events connect companies that

specialize in communications surveillance and interference to representatives of governments interested in this technology. In 2013, France welcomed TAC and Milipol. Later that year, in December, the French government announced that the export of surveillance material outside the EU would require authorization.

The Western democracies not only encourage trade in anti-freedom technology, they themselves are users. As the Special Rapporteur on Freedom of Information to the Human Rights Council stated, in his report of 3 June 2013 on internet surveillance by governments, the use of espionage technology on citizens is not limited to authoritarian regimes. No government is immune from the effects of this kind of surveillance. France, for example, reached an agreement this year with Orange. The telecommunications company. The pact grants government intelligence services complete access, free of all outside control, to the company's networks and the data that moves through them.

Development of tools designed to ensure online security for journalists and netizens

Reporters Without Borders has developed tools designed to allow information activists – journalists, bloggers and netizens – to shield themselves online,. In 2010, the organization established an ''Anti-Censorship Shelter'' for journalists, bloggers and dissidents, to teach them how to bypass censorship, protect their communications and remain anonymous online.

In addition, RWB conducts regular training sessions in digital security. The training is designed to teach journalists and bloggers how to secure their online communications using encryption, anonymous browsing and other methods. In May of this year, training was conducted in Ivory Coast for approximately 70 bloggers from Africa and elsewhere. Previously, training was carried out in Afghanistan, Egypt, Tunisia, Turkmenistan, Thailand and Senegal. And on the initiative of Privacy International, RWB and other NGOs (Human Rights Watch, Digitale Gesellschaft, FIDH, Amnesty International and Open Technology Institute) this year launched CAUSE (Coalition Against Unlawful Surveillance Exports). Its aim is to coordinate an international call for action from national governments and regional institutions, as well as raising wider awareness of the privatized surveillance industry and the damaging impact the technologies have on human rights.

However, in the absence of a specific and protective legal framework, these initiatives remain insufficient. An urgent need exists for new legal provisions, at an international, regional and national level.

Need to adopt a protective legal framework for individual internet users, and enforcement measures against ''Internet Enemies''

Some measures have already been adopted at the international level. The right to privacy is internationally recognized in the Universal Declaration on Human rights and in the International Covenant on Civil and Police Rights (Art. 12). The latter also recognizes freedom of expression (Art. 19). The Wassenaar Arrangement of July 1996 is designed to promote ''transparency and greater responsibility in transfers of conventional arms, thus preventing destabilizing accumulations.'' Forty-one countries are now parties to the agreement, among them France, Germany, the United Kingdom and the United States.

In 2011, the Human Rights Council unanimously adopted the Guiding Principles on Business and Human Rights.

The Human Rights Council also recognized on 5 July 2012, the right of free expression online, and stated that rights recognized in the physical world must likewise be recognized on the internet, regardless of national borders.

Much remains to be done. Legislation to block limitations on the free flow of information and opinion must be adopted. Because the internet is a global resource, the United Nations has a major role to play.

In light of these factors, RWB recommends that the United Nations:

- Strengthen the mandate of the ''Working Group on the Issue of Human Rights and Transnational Corporations,'' specifically authorizing it to act on individual complaints and to investigate individual cases of human rights violations linked to these companies ;

- Consider establishing an international convention concerning the responsibility of private companies in human rights matters, invoking and deepening the guiding principles of the United Nations;
- Consider establishing an international convention on the export of internet surveillance technology, authorizing controls on the furnishing of technology that endangers rights guaranteed to all internet users, establishing a monitoring agency independent of governments and capable of imposing sanctions on violators. This convention must establish rules that authorize export prohibitions in cases in which a substantial risk exists that the equipment will be used to commit or facilitate serious human rights violations.

RWB recommends that governments :

- Exercise more rigorous control on exports of internet surveillance equipment, especially to areas of armed conflict, and to governments that do not respect basic freedoms.

- Recommend that any export control regime instituted and promoted by Member States be part of an international strategy for regulating the transnational trade of surveillance technology.